International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-3, May 2014

Identification of Spoofed E-mail

Hiral Vegda, Chirag Darji

***Abstract*— Email spoofing is referred to as malicious activity in which the origin details have been altered so as to make it to appear to origin from a different source. Sending fake emails is usually used to convince the receiver so that he stays unaware of the real sender. Email spoofing may be effectively used to launch phishing attacks on the receivers. The attacker may also use the attack with some amplification and in addition use mass mailer to spam mail users. Infections may be propagated by the means of spoofed emails to attack victims. There are a variety of attackers who do email spoofing. The list starts from people trying to just have fun by sending spoofed messages to users. Other serious attacks are done by wrong doers to make damages to the systems.**

***Index Terms*—DKIM, DMARC, Email spoofing, SMTP server, SPF**

I. INTRODUCTION

Spoofing is when an e-mail message appears to come from a legitimate source but in fact is from an impostor. E-mail spoofing can be used for malicious purposes such as spreading viruses, trawling for sensitive business data and other industrial espionage activities. If you are receiving bounced (returned) emails for messages that you never sent and that use as the return address your domain and addresses you never created, then this could be a case of spoofing.

Spoofing is possibly the most frustrating abuse issue to deal with, simply because it cannot be stopped. Spoofing is similar to hand-writing many letters, and signing someone else's name to it. You can imagine how difficult that would be to trace.

II. HOW SPOOFING OCCURS

There are different ways through which spoofing occurs:

A. A spammer finds an email address or a valid domain.

B. ***A spammer sends a large email campaign with this domain*** in the From address, using various email tools that prohibit easy tracing of the origin. These tools cloak, scramble or remove the header entirely. Most people assume an email came from the address it was sent from, just as they do with the return address on snail mail they receive.

C. ***A spammer can configure his own SMTP server***

Configuration of SMTP Server can be done in the following way:

1. Go to Control Panel ➔ Administrative Tools ➔ Internet Information Services (IIS)
2. Open Properties of SMTP Server ➔Access tab ➔ Click on relay button ➔Click on Add button ➔ add the IP address of localhost.
3. Code to send the email without password of Sender's Email ID

```
System.Net.Mail.SmtpClient c = new
    SmtpClient("localhost", 25);
MailMessage m = new MailMessage(new
    MailAddress("Sender's emailid"), new
    MailAddress("Receiver's emailid"));
m.Subject ="subject";
m.Body ="body";
c.Send(m);
```

- Create an object of SMTPclient
- Create an object of mail message for sending mail.
- Send the mail to the specified email id.

4. The following mail will be generated:

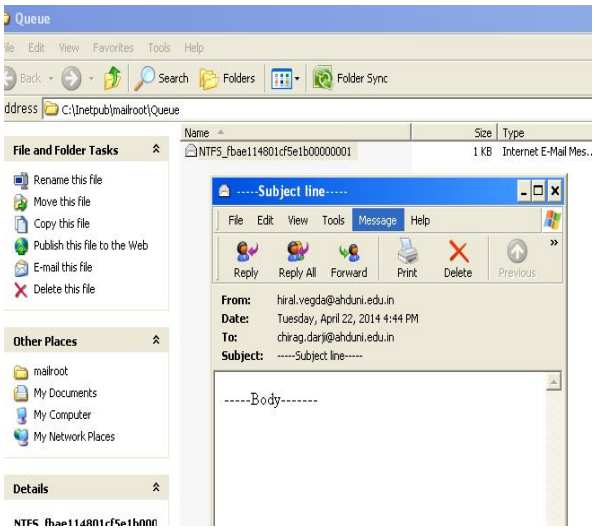

Fig 1: Generation of fake mail

Manuscript received May 23, 2014.
Hiral Vegda, School of Computer Studies, Ahmedabad University, Ahmedabad, India, 9904781373, (e-mail: hiralvegda@yahoo.com).
Chirag Darji, School of Computer Studies, Ahmedabad University, Ahmedabad, India, 9724904711, (e-mail: darjichirag.mca@gmail.com).

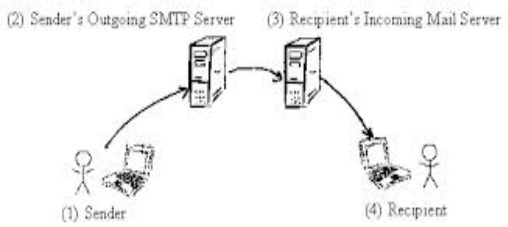

Fig 2: Process of sending mail

III. IDENTIFYING FAKE MAILS

To identify fake mails we can use any online mail tracker websites or we can do it manually.

A. *Online mail tracking websites:*

Mail tracking websites like www.emailtrackerpro.com, www.iptrackeronline.com, www.cyerforensics.in, www.ip2location.com, etc.

B. *Manual method:*

1. Bounced email alerts sometimes contain details within their message headers (in email's show original) that can help identify the messages' true origin.
   If you can see in the headers the IP address for the computer that sent the spam, you may be able to determine where the messages came from. You can then contact that PC's Internet service provider and have that IP address blocked. In the short term, that may stop the email spoofing and the bounced messages. The ISP may not help you; and even if it does, there's nothing to stop the spammer from simply spoofing your email account from a compromised PC that has a different IP address.
2. The following is the way to identify the fake mail:

   Here we have used one of the online emails tracking website like ***www.cyberforensics.in*** to track the fake mail. We have to go to the message headers in that select show original option then we have to copy the mail header and paste it to mail tracking website **www.cyberforensics.in**, then the following screen will be opened:

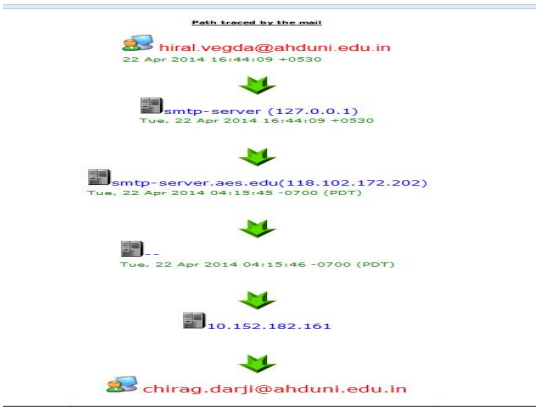

Fig 3: Path traced by the mail

Header of Actual Mail

Authentication-Results: mx.google.com;
spf=**pass** (google.com: domain of chirag.darji@ahduni.edu.in designates 2607:f8b0:400c:c01::233 as permitted sender) smtp.mail=chirag.darji@ahduni.edu.in;
dkim=**pass** header.i=@gmail.com;
dmarc=**pass** (p=NONE dis=NONE) header.from=gmail.com
Received: by mail-ve0-f179.google.com with SMTP id db12so10088658veb.10
for <chirag.darji@ahduni.edu.in>; Tue, 22 Apr 2014 09:22:29 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

Header of mail sent by SMTP

Received-SPF: **neutral** (google.com: 118.102.172.202 is neither permitted nor denied by best guess record for domain of hiral.vegda@ahduni.edu.in) client-ip=118.102.172.202;
Authentication-Results: mx.google.com;
spf=**neutral** (google.com: 118.102.172.202 is neither permitted nor denied by best guess record for domain of hiral.vegda@ahduni.edu.in) smtp.mail=hiral.vegda@ahduni.edu.in

- We have to check the received-SPF(Sender Policy Framework). So, if spf = pass then it is a permitted sender). and if spf = neutral then sender is neither permitted nor denied.
- Sender Policy Framework (SPF) is an email validation system designed to prevent email spam by detecting email spoofing, a common vulnerability, by verifying sender IP addresses. SPF allows administrators to specify which hosts are allowed to send mail from a given domain by creating a specific TXT record in the Domain Name System (DNS). Mail exchangers use the DNS to check that mail from a given domain is being sent

by a host sanctioned by that domain's administrators.

- We also have to check the dkim = pass (DomainKeys Identified Mail) which is provided by the email service provider.
- DomainKeys Identified Mail (DKIM) is a modern method of authenticating the delivery chain for email messages. It operates by signing messages with a special cryptographic signature that can be verified but not counterfeited by a third-party source. The signature, which is included in the message by a relay server in the delivery chain, proves that the message passed through that server. This helps prevent spammers and scammers from creating fraudulent messages appearing to come from that source.
- DKIM does not prevent spam from passing through a network, but it gives recipient servers confidence in the source of the message. Recipient servers can then more confidently use the reputation of the delivery network in order to judge whether a message is legitimate or not.
- Domain-based Message Authentication, Reporting and Conformance or DMARC is a method of email authentication that is a way to mitigate email abuse. It expands on two existing mechanisms, the well-known SPF and DKIM, coordinating their results on the alignment of the domain in the From: header field, which is often visible to end users. It allows specifying policies that is how to handle incoming mail based on the combined results, and to ask for reports.

IV. Conclusion

We can identify the spammer or the sender of fake mails using their IP address by checking the show original option of the message. And also using online mail tracker websites, we can identify the email server of the sender. Each email service providers are having their own authentication by reporting as phishing or spamming and they can block such kind of IP address of sender trying to send fake mails. We can also identify and report scams by reporting to the free online services.

Acknowledgment

We are very much thankful to the IJIRCST journal for giving us a chance to write paper on our area of interest. We have referred various books and online papers to get the technical knowledge to create own SMTP server.

References

[1] Dr. Wesam Bhaya , "Security against spoofing attack in mobile Ad Hoc network"
[2] Ahmad Alamgir Khan,"Preventing phishing attacks using one time password and user machine identification," International Journal of Computer Applications (0975-8887)., vol. 68-No.3, Apr. 2013.
[3] [Online]. Available: http://www.searchsecurity.techtarget.com/definition/email-spoofing
[4] [Online]. Available: http://www.pcworld.com/article/253305/minimize_your_exposure_to_email_spoofing.html
[5] [Online]. Available: http://www.fatcow.com/knowledgebase/read_article.bml
[6] [Online]. Available: http://www.consumerfraudreporting.org/spoofing.php
[7] [Online]. Available: http://www.sendblaster.com/en/support/smtp_and_sending_issues/how_configure_SMTP

Hiral Vegda: MCA, Pursuing Ph.D.

Teaching experience: More than 7 years. Teaching various subjects like Programming in C Language, Data Structures, System Software and the interested areas are Network Security, Web development applications and database.

Publications: Paper Titled "Electronic Document Security Issues: A Review" is published by International Journal of Information and Computing Technology, Research@ICT : ISTAR (Vallabh Vidhyanagar, Anand) in the January-2013 Issue

Article on "Programming Tips" is published by CSI Communications under the Section "Ask an Expert" in October-2012.

Research Work: Registered for Ph. D. to Pacific Academy of Higher Education & Research University, Udaipur.

My research area is "Strategic Approach & Intrusion Detection in Wireless Network: Issues, Challenges, Opportunities and Threats".

Membership: Member of ACM (Association for Computing Machinery) and CSI (Computer Society of India)

Activities: Various workshops conducted, coordinated and attended. Designed syllabus for the subjects Programming in C Language and Data Structures for the Ahmedabad University .

Chirag Darji: MCA

Teaching experience:I have taught Accounting and Financial Management, Web Application Development and Introduction to Visual and Windows Programming.

Membership: Member of CSI (Computer Society of India)

Activities: Various software developed, workshops conducted and attended.